In re Patent Application of
MACCHETTI ET AL.
Serial No. 09/974,705
Filed: **OCTOBER 10, 2001**
_____/

<u>In the Claims</u>:

  This listing of claims replaces all prior versions and listing of claims in the application.

  Claims 1-20 (Canceled).

  21. (Currently amended) A method of converting data between an unencrypted format and an encrypted format, the data being organized in bit words, the method comprising:
  <u>converting the data by at least</u> performing a plurality of transformation rounds comprising
   applying at least one transformation to a two-dimensional array of rows and columns of bit words defining a state array; [[and]]
   exchanging each of the rows with a respective column of the state array to form a transposed state array for at least one of the transformation rounds so that the at least one transformation is applied to the transposed state array<u>; and</u>
   <u>applying at least one round key to the state array in at least one of the transformation rounds</u>.

  22. (Previously presented) A method according to Claim 21 wherein the bit words are 8-bit words.

  23. (Previously presented) A method according to Claim 21 wherein the state array is a 4 x 4 matrix of bit words.

2

In re Patent Application of
MACCHETTI ET AL.
Serial No. 09/974,705
Filed: OCTOBER 10, 2001
———————————————————/

24.   (Previously presented) A method according to
Claim 21 wherein the plurality of transformation rounds
comprises at least 10 transformation rounds.

25.   (Previously presented) A method according to
Claim 21 wherein performing further comprises performing at
least one transformation round on a non-transposed state array.

26.   (Canceled).

27.   (Currently amended) A method according to
[[Claim 26]] Claim 21 wherein the at least one round key is
transposed before being applied to the state array.

28.   (Currently amended) A method according to
[[Claim 26]] Claim 21 further comprising adding code to
transpose the at least one round key.

29.   (Currently amended) A method according to
[[Claim 26]] Claim 21 wherein the at least one round key
comprises a plurality of round keys, each corresponding to a
respective transformation round and being applied according to
a round key schedule.

30.   (Previously presented) A method according to
Claim 29 wherein the round key schedule comprises a transposed
round key schedule.

3

In re Patent Application of
MACCHETTI ET AL.
Serial No. 09/974,705
Filed: OCTOBER 10, 2001
_____/

31.　(Currently amended)　A device for converting data between an unencrypted format and an encrypted format, the device comprising:

at least one register for storing the data in the form of bit words; and

a circuit for <u>converting the data by at least</u> performing a plurality of transformation rounds, each transformation round comprising applying at least one transformation to a two-dimensional array of rows and columns of bit words defining a state array, [[and]]

exchanging each of the rows with a respective column of the state array to form a transposed state array for at least one of the transformation rounds so that at least one transformation is applied to the transposed state array<u>, and</u>

<u>applying at least one round key to the state array in at least one of the transformation rounds</u>.

32.　(Previously presented)　A device according to Claim 31 wherein said at least one register stores bit words as 8-bit words.

33.　(Previously presented)　A device according to Claim 31 wherein said circuit operates on a state array comprising a 4x4 matrix of bit words.

34.　(Previously presented)　A device according to Claim 31 said circuit in performing a plurality of

<div style="text-align:right">Best Available Copy</div>

4

In re Patent Application of
MACCHETTI ET AL.
Serial No. 09/974,705
Filed: **OCTOBER 10, 2001**
_____/

transformation rounds performs at least 10 transformation rounds.

35. (Previously presented) A device according to Claim 31 wherein said circuit comprises at least one S-box processing module, said at least one S-box processing module operating on a group of bit words defining a cell of a column of the state array.

36. (Previously presented) A device according to Claim 35 wherein the at least one S-box processing module comprises a plurality of S-box modules, each of the plurality of S-box modules operating on a corresponding cell of a column of the state array.

37. (Previously presented) A device according to Claim 36 wherein the column of the state array comprises four cells.

38. (Previously presented) A device according to Claim 31 wherein the circuit further comprises a plurality of shift column modules, each of said plurality of shift column modules to perform a column shift operation on a column of the state array.

39. (Previously presented) A device according to Claim 38 wherein a column shift operation performed by each of said plurality of shift column modules generates shift column data, and wherein said circuit further comprises a single mix

5

In re Patent Application of
MACCHETTI ET AL.
Serial No. 09/974,705
Filed: OCTOBER 10, 2001
_____/

column module to perform column mix operations on shift column
data.

     40.   (Previously presented)   A device according to
Claim 31 wherein said circuit is an encoder for converting
data from an unencrypted data format to an encrypted data
format.

     41.   (Previously presented)   A device according to
Claim 40 wherein said circuit is an embedded system for use in
a smart card.

     42.   (Previously presented)   A device according to
Claim 31 wherein said circuit is a decoder for converting data
from an encrypted data format to an unencrypted data format.

     43.   (Previously presented)   A device according to
Claim 42 wherein said circuit is an embedded system for use in
a smart card.

     44.   (Canceled).

     45.   (Canceled).

     46.   (Canceled).

     47.   (Canceled).

     48.   (New)   A method of converting data between an
unencrypted format and an encrypted format, the data being

6

In re Patent Application of
MACCHETTI ET AL.
Serial No. 09/974,705
Filed: OCTOBER 10, 2001
_____/

organized in 8-bit words, the method comprising:

 converting the data by at least performing a
plurality of transformation rounds for converting the data
comprising

 applying at least one transformation to a two-
dimensional array of rows and columns of 8-bit words
defining a state array comprising a 4 x 4 matrix of
8-bit words,

 exchanging each of the rows with a respective
column of the state array to form a transposed state
array for at least one of the transformation rounds
so that the at least one transformation is applied
to the transposed state array,

 applying at least one round key to the state
array in at least one of the transformation rounds.

 49.   (New) A method according to Claim 48 wherein
the at least one round key is transposed before being applied
to the state array.

 50.   (New) A method according to Claim 48 further
comprising adding code to transpose the at least one round
key.

 51.   (New) A method according to Claim 48 wherein
the at least one round key comprises a plurality of round
keys, each corresponding to a respective transformation round
and being applied according to a round key schedule.

7